7. (Amended) A method for efficient encryption and decryption of Internet, Intranet, or e-mail messages, comprising the steps of:

providing a sending unit in communication with an integrated encryption circuit embedded with an encryption algorithm;

encrypting a message at said sending unit;

appending to the message at said sending unit a receiver's unencrypted IP address;

appending to said message a receiver's encrypted IP address;

sending said encrypted message with said unencrypted IP address and said encrypted IP address to a receiving unit;

providing said receiving unit having an integrated encryption circuit embedded with an decryption algorithm;

receiving with said receiving unit said encrypted message with said unencrypted IP address and said encrypted IP address;

decrypting with said receiving unit said encrypted IP address, thereby resulting in a decrypted IP address;

storing said decrypted IP address in a first register built into said integrated encryption circuit within said receiving unit;

storing said unencrypted IP address into a second register built into said integrated encryption circuit within receiving unit;

means for comparing said second register storing unencrypted IP address to said first register storing said decrypted IP address;

decrypting said message if said second register storing unencrypted IP address matches said first register storing said decrypted IP address; and

means for halting decryption process if said second register storing unencrypted IP address does not match said first register storing said decrypted IP address.

8. (New) A method of encrypting Internet, Intranet, or e-mail messages, comprising:

providing a communication device in communication with a private encryption key generator;

generating a primary private encryption key;

encrypting data with said primary private encryption key;

providing a public encryption key and second private encryption key pair;

encrypting said primary private encryption key and with a public/second private encryption key pair; and

sending said data encrypted with said primary private encryption key and said primary private encryption key encrypted with said public/second private encryption key pair to a receiving unit.

9. (New) The method of claim 8, wherein access to said private encryption key generator is password controlled.

10. (New) The method of claim 9 wherein said password is user defined.

11. (New)The method of claim 8 wherein said encryption key generator is located within a communication device.

12. (New) The method of claim 8 wherein said primary private encryption key is randomly generated.

13. (New) A method of decrypting Internet, Intranet, or e-mail messages, comprising:

providing a communication device in communication with a private encryption key generator;

receiving an encrypted message with said communication device, said message having data encrypted with a primary private encryption key and a primary private encryption key encrypted with a public/second private encryption key pair;

providing access to said private encryption key generator;

decrypting said public/second private encryption key pair with said private encryption key generator, thereby providing said primary private encryption key; and

decrypting said data with said primary private encryption key.

14. (New) The method of claim 13 wherein access to said private encryption key generator is password controlled.

15. (New) The method of claim 14 wherein said password is user defined.

16. (New) The method of claim 13 wherein access to said primary encryption key generator is requires verification.

17. (New) The method of claim 16 wherein said verification comprises a Certification of Authority.

18. (New) A method of encrypting Internet, Intranet, or e-mail messages, comprising the steps of:

providing a communication device in communication with an integrated encryption circuit embedded with encryption algorithms;

accessing said integrated encryption circuit to encrypt a message;

encrypting said with said encryption algorithms;

providing a message header comprising a sender's private cypher key and a digital bit array;

encrypting said message header using a receiver's public encryption key;

appending said encrypted message header to said encrypted message; and

transmitting said encrypted message header and said encrypted message to a receiver.

19. (New) The method of claim 18 wherein said message is transmitted through an Internet.

20. (New) The method of claim 18 wherein said message is transmitted through an Intranet.

21. (New) The method of claim 18 wherein said message is transmitted through an e-mail.

22. (New) The method of claim 18 wherein said message is transmitted through a wireless communication system.

23. (New) A method decrypting a message of claim 18 further comprising the steps of:

providing a communication device in communication with a integrated decryption circuit;

receiving an encrypted message and encrypted message header with said communication device;

accessing said integrated decryption circuit to decrypt said encrypted message and message header;

decrypting said message header with said decryption circuit;

validating said message header with said decryption circuit;